(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 935 214 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
11.08.1999 Patentblatt 1999/32

(51) Int Cl.[6]: **G06K 19/073**

(21) Anmeldenummer: **99200263.4**

(22) Anmeldetag: **29.01.1999**

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: **06.02.1998 DE 19804784**

(71) Anmelder:
- **Philips Patentverwaltung GmbH**
  22335 Hamburg (DE)
  Benannte Vertragsstaaten:
  DE
- **Koninklijke Philips Electronics N.V.**
  5621 BA Eindhoven (NL)
  Benannte Vertragsstaaten:
  FR GB IT

(72) Erfinder: **Rabeler, Thorwald**
22335 Hamburg (DE)

(74) Vertreter: **Peters, Carl Heinrich, Dipl.-Ing.**
Philips Patentverwaltung GmbH,
Röntgenstrasse 24
22335 Hamburg (DE)

(54) Chipkarte mit integrierter Schaltung

(57) Chipkarten mit Mikroprozessor und Speicher werden für verschiedene Anwendungsfälle eingesetzt. Gewünscht ist auch, daß dieselbe Chipkarte für verschiedene Anwendungen verwendet werden kann. Dazu ist es erforderlich, daß die verschiedenen Benutzerprogramme sicher voneinander getrennt sind und ein gegenseitiger Zugriff nicht möglich ist. Dies wird insbesondere durch die Aufteilung in einen System-Mode, in dem alle Zugriffsrechte freigegeben sind, und in einen Benutzer-Mode erreicht, der über ein bestimmtes Bit im Programmstatuswort eingestellt wird. Dieses Mode-Bit steuert u.a. eine Trennung in dem Bus für die Register für spezielle Funktionen, so daß bestimmte Register in Benutzer-Mode nicht zugänglich sind. In diesen Registern können Informationen enthalten sein, die den Zugriff auf nur bestimmte Speicherbereiche freigeben, so daß im Benutzer-Mode dieser Zugriff nicht geändert werden kann. Ferner kann jedes Speicherwort eine individuell einem Anwenderprogramm zugeordnete Prüfinformation enthalten, die beim Auslesen mit der entsprechenden Prüfinformation verglichen wird, wobei bei fehlender Übereinstimmung die ausgelesene Information intern nicht weitergeleitet wird.

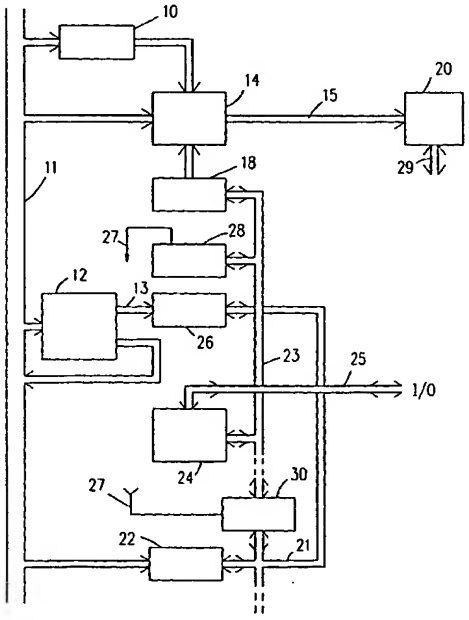

Fig.1

EP 0 935 214 A2

Beschreibung

[0001] Die Erfindung betrifft eine Chipkarte mit einer integrierten Schaltung, die eine Steuereinheit in Form eines Mikroprozessors und Speicher enthält. Derartige Chipkarten sind allgemein bekannt und werden für verschiedene Zwecke verwendet. In häufigen Fällen werden solche Scheckkarten für Zwecke verwendet, in denen sich auf der Karte sicherheitsrelevante Informationen befinden. Dies ist beispielsweise der Fall bei Bankkarten, bei denen sich auf der Scheckkarte Guthaben oder Kreditlinien befinden sowie persönliche Geheimzahlen, oder bei Patientenkarten, auf denen sich vertrauliche Informationen über den Patienten befinden, die beispielsweise nur nach Eingabe einer persönlichen Geheimnummer auslesbar sein sollen. Ferner werden solche Karten als Zugangskontrolle für bestimmte Räume oder Gebäude verwendet. In allen Fällen soll verhindert werden, daß durch betrügerische Manipulationen geheime Daten aus der Karte ausgelesen werden können oder daß Daten auf der Karte in unerwünschter Weise verändert werden können.

[0002] Aufgabe der Erfindung ist es, eine Chipkarte mit Mikroprozessor und Speicher anzugeben, bei der ein unzulässiger, d.h. nicht gewünschter Zugriff auf Daten in der Karte zum Auslesen oder Verändern mit möglichst großer Sicherheit verhindert wird.

[0003] Diese Aufgabe wird erfindungsgemäß im wesentlichen dadurch gelöst, daß im Programmstatuswort-Register, dem PSW-Register, wenigstens ein Mode-Bit vorhanden ist, dessen Wert einen Benutzer-Mode oder einen System-Mode angibt. Im Benutzer-Mode ist durch den entsprechenden Bitwert des Mode-Bits der Zugriff auf wenigstens Teile des PSW-Registers sowie auf alle solchen Register- und Speichersegmente, die nur im System-Mode verwendet werden, gesperrt. Dadurch ist der Zugriff auf alle solchen Register und Speicher, in denen sich sicherheitsrelevante Informationen befinden, nur im System-Mode möglich. Der System-Mode arbeitet mit einem fest gespeicherten Programm, das selbstverständlich ebenfalls von außerhalb weder auslesbar noch veränderbar ist. Dieses Programm ist unabhängig von den jeweiligen Anwendungsfällen.

[0004] Dies hat den Vorteil, daß ein solches System-Programm nur einmal auf seine sicherheitsrelevanten Funktionen geprüft und freigegeben werden muß. Die Anwenderprogramme, die von den entsprechenden Institutionen wie Banken oder Krankenkassen erstellt und auf die Karte gebracht werden, brauchen dann nicht besonders geprüft zu werden. Jeder Zugriff auf geheime Daten im Rahmen eines Anwenderprogramms erfolgt ausschließlich über das System-Programm. Dies ist besonders wichtig auch für Chipkarten, die mehr als einer Anwendung dienen. Durch das System-Programm wird sichergestellt, daß alle verschiedenen Anwenderprogramme eindeutig und zuverlässig voneinander getrennt sind und nicht von einem Anwenderprogramm auf ein anderes bzw. auf darin verwendete Daten zugegriffen werden kann.

[0005] Zum Zugriff auf geheime Daten, die in einem Anwenderprogramm rechtmäßig verwendet werden sollen, wird stets ein bestimmter Sprung in das System-Programm ausgelöst, der das Mode-Bit umschaltet. Im System-Mode sind alle Register und alle Speicherplätze zugänglich. Andererseits kann im System-Mode aber genau geprüft werden, ob der gewünschte Zugriff tatsächlich zulässig ist. Diese Prüfung kann auch durch einen betrügerischen Benutzer nicht ausgeschaltet werden. Einen Zugriff auf geheime Daten ist auch jede Eingabe- und Ausgabeoperation von Daten gleichgestellt.

[0006] Die Sperrung von Speicherplätzen bzw. die Freigabe bestimmter Speicherplatzbereiche für jeweils ein Anwenderprogramm wird auf einfache Weise dadurch erreicht, daß der Speicher in bestimmte Bereiche unterteilt ist, die auch mit Segmenten oder Seiten bezeichnet werden, und unterschiedlichen Anwenderprogrammen sind dann zweckmäßig auch unterschiedliche Segmente zugeordnet. Die Segmente werden durch den Inhalt eines bzw. mehrerer entsprechende Register bestimmt, die nur im System-Mode veränderbar sind. Dadurch sind Speicherbereiche verschiedener Anwenderprogramme sicher gegeneinander abgegrenzt.

[0007] Zusätzlich kann innerhalb eines Segments der Zugriff auf nur einen Teil dieses Segments freigegeben werden, indem zusätzliche Register für eine Angabe einer Grenzadresse innerhalb eines Segments vorgesehen werden. Jede Adresse, d.h. die Bits geringerer Wertigkeit, werden automatisch mit dem Inhalt eines solchen Registers verglichen. Auch diese Register können nur im System-Mode gelesen und überschrieben werden.

[0008] Ferner ist, vorzugsweise im Segmentregister, eine Bitgruppe vorgesehen, deren Wert zusammen mit eingeschriebenen Daten in den Speicherplatz mit eingeschrieben wird. Beim Auslesen wird dann geprüft, ob der Inhalt des entsprechenden Bereichs der Speicherstelle mit dieser Bitgruppe übereinstimmt. Falls dies nicht der Fall ist, wird das Auslesen gesperrt.

[0009] Wenn von einem Benutzerprogramm im Benutzer-Mode auf ein Register oder einen Speicherplatz zugegriffen werden soll, der in diesem Benutzerprogramm nicht zulässig ist, kann anstelle einer besonderen Systemmeldung nur ein Wert ausgegeben werden, der einer leeren Speicherzelle entspricht, die also nach Herstellung der Karte nicht beschrieben worden ist. Auf diese Weise kann ein betrügerischer Benutzer nicht erkennen, ob er tatsächlich auf einen leeren Speicherplatz oder auf einen gesperrten Speicherplatz zugreifen wollte. Außerdem entspricht ein solcher Wert einem unbedingten Sprung in den System-Mode.

[0010] Die Sperrung aller nicht zugelassenen Speicherbereiche erfolgt also über Register, die nur im System-Mode veränderbar sind. Diese Register bilden wenigstens einen Teil der Register für spezielle Funktionen, der sogenanten SF-Register. Diese Register sind über einen registerinternen Bus miteinander verbun-

den. Außerdem hat dieser interne Registerbus eine Schnittstelle zum internen Datenbus, über die Daten vom Datenbus in die Register eingeschrieben oder aus den Registern zum Datenbus ausgelesen werden können. Zweckmäßig wird nun dieser Registerbus durch einen Schalter unterteilt, der nur im System-Mode geschlossen ist. Dies ist eine sehr einfache Möglichkeit, die entsprechenden Register und indirekt damit auch alle nicht zugänglichen Speicherplätze zu sperren.

[0011] Ausführungsbeispiele der Erfindung werden nachfolgend anhand der Zeichnung erläutert. Es zeigen:

Fig. 1 ein Blockschaltbild der wichtigsten Teile eines Mikroprozessors für eine Chipkarte,
Fig. 2 den genaueren Aufbau eines Details daraus,
Fig. 3 ein Blockschaltbild für die Überprüfung von Adreßgrenzen,
Fig. 4 ein Blockschaltbild für die Prüfung des Inhalts von Speicherplätzen,
Fig. 5 eine symbolische Darstellung der Unterteilung zwischen geschütztem SystemBereich und ungeschütztem Benutzer-Bereich,
Fig. 6 ein Beispiel für den Aufbau eines Programmstatusworts in zwei getrennten Registern.

[0012] Die Fig. 1 zeigt schematisch die für die Erfindung wesentlichen Teile eines Mikroprozessors. An einen internen Bus 11, der eine Anzahl Daten- und Steuerleitungen umfaßt, ist ein Programmzähler 10 angeschlossen, der über den Datenbus auf eine bestimmte Adresse gesetzt werden kann und im übrigen autonom weiterzählt. Die dafür notwendigen Steuersignale sind beim Programmzähler sowie bei den übrigen Elementen in dieser Figur sowie in den anderen Figuren der Übersichtlichkeit halber nicht einzeln dargestellt.

[0013] Der Programmzähler 10 liefert seinen Inhalt an eine Speicherverwaltungseinheit MMU 14, die über eine Verbindung 15 einen Speicher 20 mit Adressen- und Steuersignalen versorgt. Dieser Speicher 20 besteht zweckmäßig aus mehreren Speichereinheiten, nämlich insbesondere einem ROM für das Systemprogramm bzw. wesentliche Teile davon, einem beschreibbaren EEPROM für Anwenderprogramme und bestimmte feste Daten wie Geheimnummern sowie aus einem flüchtigen RAM insbesondere zur Speicherung von Zwischenergebnissen bei einzelnen Verarbeitungsschritten. Die Auswahl der einzelnen Speicher geschieht durch Steuersignale über die Verbindung 15. Über eine Verbindung 29 werden aus adressierten Speicherplätzen ausgelesene Daten abgegeben bzw. in beschreibbare Speicherplätze einzuschreibende Daten zugeführt.

[0014] Die MMU14 ist ferner direkt mit dem Bus 11 verbunden, um Daten vom Bus 11 als Adressen dem Speicher 20 zuzuführen. Außerdem ist die MMU14 mit Registern 18 verbunden, die hier vereinfacht als ein Block dargestellt sind und die Angaben enthalten, welche Speichereinheit im Speicher 20 auszuwählen ist und zusätzlich, welcher Speicherbereich bzw. Adreßbereich in der ausgewählten Speichereinheit angesprochen wird. Dazu ist insbesondere die EEPROM-Speichereinheit in Bereiche unterteilt, die allgemein als Segmente oder Seiten bezeichnet werden. Jedem Anwenderprogramm werden ein oder mehrere bestimmte Segmente für Programminformationen und Daten zugeordnet, die beim Einschreiben des betreffenden Anwenderprogramms festgelegt werden. Diese Zuordnungen können lediglich durch das Systemprogramm verändert werden, wie spätert erläutert wird.

[0015] Eine arithmetisch-logische Einheit ALU12 ist mit einem Eingang mit dem Bus 11 verbunden. Der interne Aufbau dieser Einheit, der insbesondere eine Recheneinheit und einen Akkumulator sowie weitere Register umfaßt, ist an sich bekannt und daher hier nicht weiter dargestellt. Die Rechenergebnisse dieser Einheit 12 werden wieder auf den Bus 11 zurückgeführt. Außerdem werden einige Signale, die bei der Durchführung von Berechnungen auftreten, wie Übertragssignale, Überlaufmeldungen oder Null-Werte, über eine Verbindung 13 einem Register 26 zugeführt, das einen Teil des sogenannten Programmstatusworts enthält. Der zweite Teil des Programmstatusworts ist in einem Register 28 enthalten.

[0016] Für die Eingabe oder Ausgabe von Daten, beispielsweise von außerhalb der Chipkarte oder von einem Koprozessor in der Chipkarte bzw. auf demselben Chip wie der Mikroprozessor, sind Register 24 vorgesehen, die über eine Verbindung 25 von außerhalb des Mikroprozessors geladen werden können oder nach außerhalb Daten abgeben können.

[0017] Die Register 18, 28 und 24 sind über einen speziellen Bus 23 miteinander verbunden, der auf eine Verbindungseinheit 30 führt. An diesen Bus 23 können noch weitere Register angeschlossen sein, wie durch die gestrichelte Linie zur Verbindungseinheit 30 angedeutet ist. Die Verbindungseinheit 30 ist ferner mit einem internen Bus 21 verbunden, der auf das Register 26 für den einen Teil des Programmstatusworts sowie auf eine Koppeleinheit 22 führt, die diesen Bus 21 mit dem Bus 11 bei entsprechender Ansteuerung über nicht gesondert dargestellte Steuerleitungen verbindet. Die Busse 21 und 23 stellen den in Mikroprozessoren üblichen internen Bus für die Register für spezielle Funktionen dar. Diese beiden Teile bilden einen einheitlichen Bus, wenn die Verbindungseinheit 30 durch Ansteuerung über die Leitung 27 die beiden Busteile verbindet.

[0018] Die Steuerleitung 27 ist mit einem bestimmten Teil des Registers 28 verbunden, der ein Mode-Bit enthält. Der Wert dieses Bits bestimmt, ob der Mikroprozessor im System-Mode oder im Benutzer-Mode arbeitet. Wenn der Wert dieses Bits den System-Mode angibt, wird die Verbindungseinheit 30 angesteuert, um beide Busteile 21 und 23 miteinander zu verbinden, so daß dann ein einheitlicher Bus hergestellt wird, über den alle Register für spezielle Funktionen, wie die darge-

stellten Register 18, 24, 26 und 28 sowie gegebenenfalls weitere, nicht dargestellte Register miteinander verbunden sind. Im System-Mode kann also auf alle Register zugegriffen werden. Im Benutzer-Mode wird durch den entsprechenden anderen Wert des Mode-Bits über die Steuerleitung 27 die Verbindungseinheit 30 angesteuert, um die beiden Busteile 21 und 23 zu trennen. Nun kann nicht mehr auf die Register 18, 28 und 24 sowie weitere am Bus 23 angeschlossene Register zugegriffen werden, und zwar weder zum Schreiben noch auch nur zum Lesen.

[0019] Der Übergang vom Benutzer-Mode in den System-Mode geschieht durch einen besonderen Sprungbefehl, durch den das Mode-Bit im Register 28 auf den System-Mode umgeschaltet wird. Gleichzeitig wird der Anfang des System-Programms aufgerufen, dessen wesentlicher Inhalt unveränderlich festgelegt ist. Im System-Programm kann beispielsweise das Register 18 verändert werden, um andere Speichereinheiten oder andere Segmente in einer Speichereinheit im nachfolgenden Anwenderprogramm adressieren zu können. Am Schluß des System-Programms wird im Register 28 das Mode-Bit wieder zurückgeschaltet, und damit wird über die Steuerleitung 27 in der Verbindungseinheit 30 wieder die Verbindung zum Bus 23 unterbrochen, so daß dann kein Zugriff auf die daran angeschlossenen Register möglich ist.

[0020] In Fig. 2 ist der Aufbau der Verbindungseinheit 30 etwas detaillierter dargestellt. Die Übertragung von Daten vom Bus 21 zum Bus 23 erfolgt über einen Schalter 302, während die vom Bus 23 zum Bus 21 zu übertragenden Daten über einen Schalter 304 führen. Die Schalter 302 und 304 werden gemeinsam über die Steuerleitung 27 angesteuert. In der in Fig. 2 dargestellten Stellung der Schalter 302 und 304 ist die Verbindung unterbrochen, und zum Bus 21 werden Daten übertragen, die von einer Leitung 306 mit festem Datenwert kommen. Dieser Datenwert entspricht beispielsweise dem Wert des Sprungbefehls, mit dem in den System-Mode gesprungen wird. Wenn also in einem Benutzerprogramm verbotener Weise auf ein nicht zugelassenes Register zugegriffen werden soll, wird also ein Wert entsprechend dem Sprungbefehl ausgelesen. Wenn dieser Wert als Befehl interpretiert werden soll, erfolgt bei einem solchen verbotenen Zugriff also immer ein Sprung in den System-Mode, in dem nur festgelegte, von einem Benutzer nicht veränderbare Befehlsfolgen ablaufen.

[0021] In Fig 3 sind einige Teile der MMU 14 näher dargestellt. Die Verbindung zum Bus 11 führt auf einen Adreßrechner 140, wo die Daten vom Bus 11 als Adresse mit einem über die Verbindung 19 vom Register 18 in Fig. 1 kommenden Adreßteil höherer Wertigkeit verknüpft und über die Verbindung 141 ausgegeben werden. Die Verbindung 141 führt auf eine Blockiereinheit 144 und einen Vergleicher 142. Ein zweiter Eingang des Vergleichers 142 ist mit dem Ausgang eines Registers 32 verbunden, das ebenfalls als Register für spezielle Funktionen mit dem Bus 23 verbunden ist, der nur im System-Mode zugänglich ist und in diesem System-Mode mit einem Wert für eine Adreß-Grenze geladen werden kann. Diese Adreß-Grenze wird mit vorzugsweise Teilen der Adresse auf der Verbindung 141 verglichen, und wenn die Adresse innerhalb der vorgegebenen Grenze liegt, wird vom Vergleicher 142 über die Leitung 141 die Blockiereinheit 144 freigegeben und die Adresse über die Verbindung 15 dem Speicher 20 in Fig. 1 zugeführt. Auf diese Weise kann im Benutzer-Mode der Zugriff auf einen Teil eines dem betreffenden Benutzerprogramm zugeordneten Segments gesperrt werden.

[0022] Eine weitere Sicherung gegen Zugriff auf nicht erlaubte Daten ist in Fig. 4 schematisch dargestellt. Wenn aus dem Speicher 20 in Fig. 1 der Inhalt eines Speicherplatzes ausgelesen und die entsprechenden Daten über die Verbindung 29 abgegeben werden, werden diese einem Vergleicher 42 und einer weiteren Blockiereinheit 40 zugeführt. Der Vergleicher 42 erhält an einem weiteren Eingang Daten aus dem Register 18, das über den Bus 23 geladen wurde. Der Vergleicher 42 prüft bestimmte Teile des Datenworts auf der Verbindung 29 auf Gleichheit mit den vom Register 18 zugeführten Daten. Nur bei Gleichheit wird über die Leitung 43 die Blockiereinheit 40 freigegeben und die Daten auf der Verbindung 45 abgegeben. Diese Daten werden abhängig von entsprechenden Steuersignalen auf nicht gesondert dargestellten Steuerleitungen in ein Datenregister 44 eingeschrieben, das diese Daten dem Bus 11 zuführt, oder in Befehlsregister 46, das diese Daten als Befehl einem nicht dargestellten Befehlsdekoder zuführt.

[0023] Wenn vom Bus 11 über das Datenregister 44 Daten in den Speicher 20 in Fig. 1 eingeschrieben werden sollen, gehen diese ebenfalls über die Blockiereinheit 40 und werden dort um Daten entsprechend dem Inhalt des Registers 18 ergänzt und über die Verbindung 29 in den Speicher 20 eingeschrieben. Dadurch wird beim Auslesen dieser Daten in dem zugehörigen Benutzerprogramm die erforderliche Gleichheit mit dem Inhalt des Registers 18 festgestellt. In einem anderen Benutzerprogramm, in dem diese Prüfdaten einen anderen Wert haben, kann also nicht auf Daten eines fremden Benutzerprogramms zugegriffen werden.

[0024] In Fig. 5 ist symbolisch die Aufteilung in einen geschützten Systemteil 50 und einen ungeschützten Benutzerteil 60 dargestellt. Im Benutzerteil 60 ist der Zugriff auf einen Stapelspeicher 62 und den Programmzähler 64 freigegeben. Außerdem steht diesem Benutzerteil eine Hälfte des Registers 59 für das Programmstatuswort zur Verfügung. Der andere Teil dieses Registers 59 steht nur dem Systemteil 50 zur Verfügung. Darin kann über Register 57 auf System-Stapelspeicher 570, 571 zugegriffen werden, außerdem über eine Schnittstelle 52 auf den Bus für die Register für spezielle Funktionen, wie ein Register 56 für die Steuerung der Schreibfreigabe in Speicher und das Register 55 für überhaupt den Zugriff auf Speicher sowie das Register 54 für Eingabe/Ausgabe-Operationen und ein Register

53 für einen Koprozessor, der vorzugsweise auf demselben Chip angeordnet ist. Es können noch weitere derartige, nicht dargestellte Register vorhanden sein.

[0025] Der Systembereich 50 mit den Zugriffsmöglichkeiten auf die darin angedeuteten Einheiten ist nur möglich, wenn das Mode-Bit gesetzt ist. Im Benutzer-Bereich ist der Zugriff auf die darin dargestellten Einheiten 62 und 64 möglich, jedoch nicht auf die im Systembereich 50 dargestellten Einheiten.

[0026] In Fig. 6 ist ein Beispiel für den Aufbau eines Programmstatusworts 70 dargestellt. Der Abschnitt 71 enthält das Mode-Bit. Im Abschnitt 72 befindet sich ein Bit, mit dessen Hilfe der Programmablauf überprüft werden kann, was insbesondere bei der Erstellung von Programmen wichtig ist. Der Inhalt des Abschnitts 73 dient der Registerauswahl. Mit dem Inhalt des Abschnitts 74 werden Unterbrechungsanforderungen maskiert. Diese Abschnitte gehören zu derjenigen Hälfte des Programmstatusworts, das nur im System-Mode veränderbar ist.

[0027] Der Teil nach dem Doppelstrich ist auch im Benutzer-Mode lesbar und veränderbar und enthält zwei Abschnitte 75 und 76, in denen Übertragssignale gespeichert werden, die in der ALU12 in Fig. 1 entstehen. Der Abschnitt 77 kann weitgehend frei vom Benutzerprogramm definiert werden. Im Abschnitt 78 wird die Meldung gespeichert, daß in der ALU12 in Fig. 1 ein Überlauf aufgetreten ist. Der Abschnitt 79 gibt an, daß in der ALU12 ein negatives Ergebnis aufgetreten ist, und der Abschnitt 80 gibt an, daß der Wert Null bei der Berechnung entstanden ist. Da dies nur Signale der ALU12 in Fig. 1 sind, muß der Zugriff auf diese Bereiche auch im Benutzer-Mode möglich sein.

Patentansprüche

1. Chipkarte mit einer integrierten Schaltung, die eine Steuereinheit in Form eines Mikroprozessors und wenigstens einen Speicher mit einer Vielzahl über Adressen zugreifbarer Speicherplätze enthält, wobei der Mikroprozessor mehrere Register umfaßt, von denen mindestens ein PSW-Register ein Programmstatuswort enthält, in dem der Wert wenigstens eines vorgegebenen Mode-Bits einen Benutzer-Mode oder einen System-Mode bestimmt, wobei der Zugriff auf wenigstens Teile des PSW-Registers sowie auf alle solchen Register und auf Speichersegmente, die nur im System-Mode verwendet werden, bei einem den Benutzer-Mode angebenden Mode-Bit gesperrt ist.

2. Chipkarte nach Anspruch 1, wobei das PSW-Register aus wenigstens einem ersten und einem zweiten Teilregister besteht und das erste Teilregister das Mode-Bit sowie eine Information zur Auswahl eines von mehreren Register-Blöcken enthält und nur im System-Mode lesbar und veränderbar ist.

3. Chipkarte nach Anspruch 1 oder 2, wobei jede im Benutzer-Mode auftretende Unterbrechungsanforderung einen Sprung in den System-Mode auslöst, der das Mode-Bit umschaltet, und alle Register, die für Eingabe/Ausgabe-Operationen und für die Steuerung von mit dem Mikroprozessor gekoppelten Steuerschaltungen dienen, nur im System-Mode verwendet werden.

4. Chipkarte nach einem der vorhergehenden Ansprüche, wobei wenigstens eines der Register ein erstes Segment-Adressen-Register ist, das die Adresse eines Speichersegments enthält, in dem Daten für das momentan ausgeführte Programm enthalten sind, und wenigstens ein weiteres Register ein zweites Segment-Adressen-Register ist, das die Adresse eines vorzugsweise anderen Speichersegments enthält, und im Benutzer-Mode eine Veränderung des ersten und des zweiten Segment-Adressen-Registers gesperrt ist.

5. Chipkarte nach einem der vorhergehenden Ansprüche, wobei weitere Register Adreß-Register sind, die je eine Adresse innerhalb eines vom Segmentadressen-Register angegebenen Speicherbereichs angeben, wobei jedem Adreß-Register ein Hilfs-Adreßregister zugeordnet ist, das nur im System-Mode veränderbar ist und wenigstens die höchstwertigen Bits der Adresse sowie eine Prüfinformation enthält, und wobei ein Vergleicher vorgesehen ist, der die Prüfinformation des Hilfs-Adreßregisters mit aus vorgegebenen Bitstellen des adressierten Speicherplatzes ausgelesenen Informationen vergleicht und im Benutzer-Mode nur bei Übereinstimmung der Prüfinformation mit der ausgelesenen Information die Weiterleitung der aus dem adressierten Speicherplatz ausgelesenen Information oder eine Veränderung der Information des adressierten Speicherplatzes freigibt.

6. Chipkarte nach einem der vorhergehenden Ansprüche, wobei von einem im Benutzer-Mode adressierten Register, das nur im System-Mode verwendet wird, nur ein vorgegebenes Bitmuster, vorzugsweise das Bitmuster eines nach der Herstellung der integrierten Schaltung nicht veränderten Speicherplatzes, weitergeleitet wird.

7. Chipkarte nach einem der vorhergehenden Ansprüche, wobei die Register über einen Bus mit der übrigen Schaltung des Mikroprozessors derart verbunden sind, daß die nur im System-Mode verwendeten Register am vom Mikroprozessor abgewandten Ende des Busses angeordnet sind, und in dem Bus vor diesem Register ein nur vom Mode-Bit gesteuertes Sperrgatter angeordnet ist.

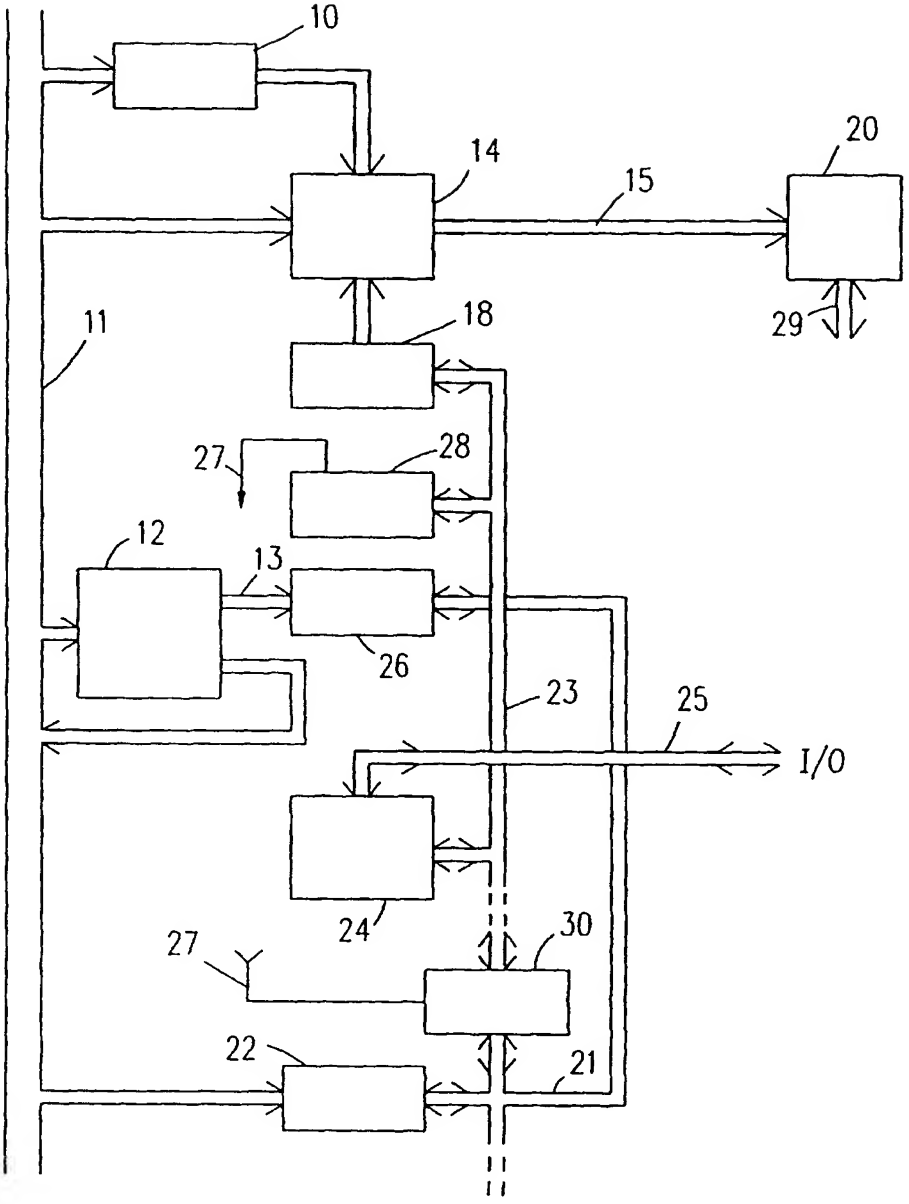

Fig.1

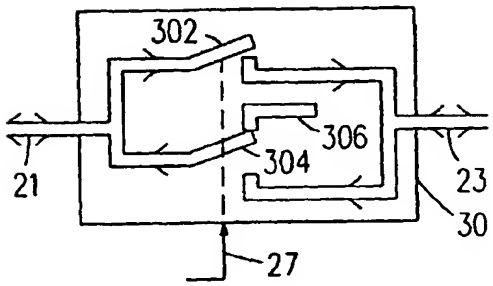

Fig.2

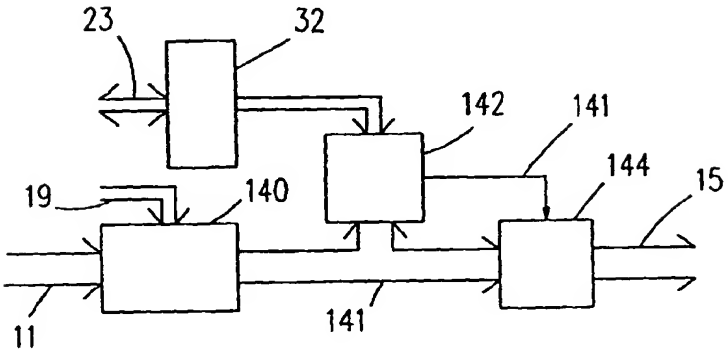

Fig.3

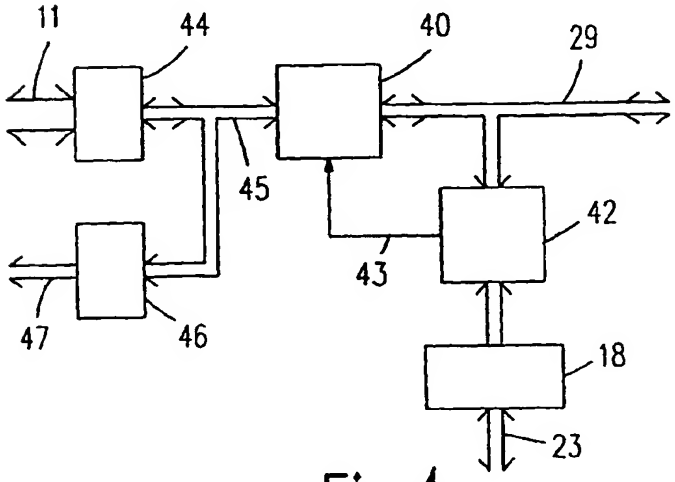

Fig.4

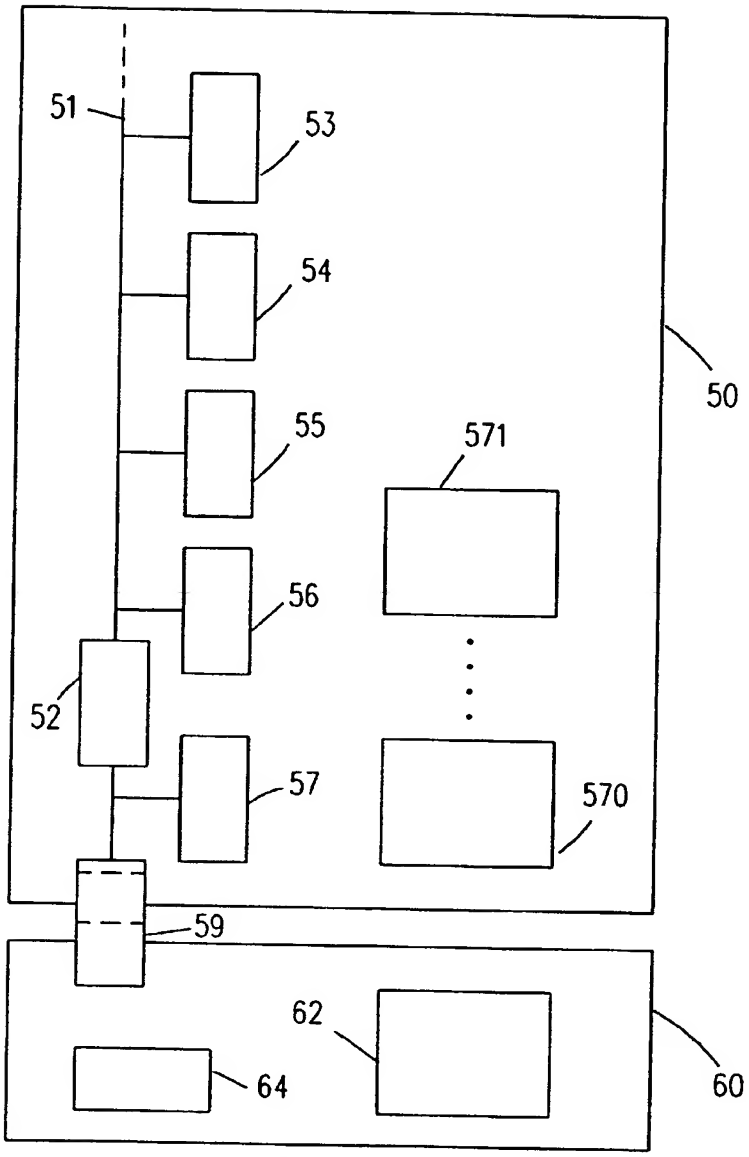
51
53
54
50
55
571
56
52
57
570
59
62
64
60

Fig.5

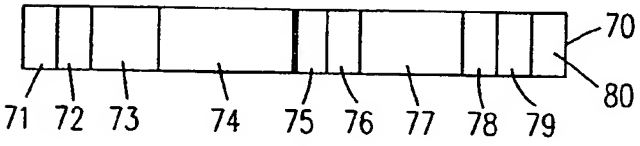
70
80
71
72
73
74
75
76
77
78
79

Fig.6

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 935 214 A3

(12) EUROPÄISCHE PATENTANMELDUNG

(88) Veröffentlichungstag A3:
14.08.2002 Patentblatt 2002/33

(43) Veröffentlichungstag A2:
11.08.1999 Patentblatt 1999/32

(21) Anmeldenummer: **99200263.4**

(22) Anmeldetag: **29.01.1999**

(51) Int Cl.[7]: **G06K 19/073**, G07F 7/10

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: **06.02.1998 DE 19804784**

(71) Anmelder:
- **Philips Corporate Intellectual Property GmbH**
  52064 Aachen (DE)
  Benannte Vertragsstaaten:
  DE
- **Koninklijke Philips Electronics N.V.**
  5621 BA Eindhoven (NL)
  Benannte Vertragsstaaten:
  FR GB IT

(72) Erfinder: **Rabeler, Thorwald**
22335 Hamburg (DE)

(74) Vertreter: **Peters, Carl Heinrich, Dipl.-Ing.**
Philips Corporate Intellectual Property GmbH,
Habsburgerallee 11
52064 Aachen (DE)

(54) Chipkarte mit integrierter Schaltung

(57) Chipkarten mit Mikroprozessor und Speicher werden für verschiedene Anwendungsfälle eingesetzt. Gewünscht ist auch, daß dieselbe Chipkarte für verschiedene Anwendungen verwendet werden kann. Dazu ist es erforderlich, daß die verschiedenen Benutzerprogramme sicher voneinander getrennt sind und ein gegenseitiger Zugriff nicht möglich ist. Dies wird insbesondere durch die Aufteilung in einen System-Mode, in dem alle Zugriffsrechte freigegeben sind, und in einen Benutzer-Mode erreicht, der über ein bestimmtes Bit im Programmstatuswort eingestellt wird. Dieses Mode-Bit steuert u.a. eine Trennung in dem Bus für die Register für spezielle Funktionen, so daß bestimmte Register in Benutzer-Mode nicht zugänglich sind. In diesen Registern können Informationen enthalten sein, die den Zugriff auf nur bestimmte Speicherbereiche freigeben, so daß im Benutzer-Mode dieser Zugriff nicht geändert werden kann. Ferner kann jedes Speicherwort eine individuell einem Anwenderprogramm zugeordnete Prüfinformation enthalten, die beim Auslesen mit der entsprechenden Prüfinformation verglichen wird, wobei bei fehlender Übereinstimmung die ausgelesene Information intern nicht weitergeleitet wird.

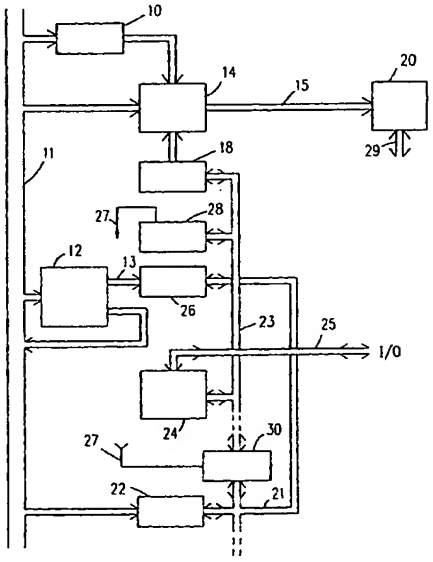

Fig.1

EP 0 935 214 A3

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 99 20 0263

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.6)
A	EP 0 512 542 A (GAO GES AUTOMATION ORG) 11. November 1992 (1992-11-11) * Spalte 1, Zeile 55 - Spalte 3, Zeile 51 * * Abbildung 2 *	1,2,5	G06K19/073 G07F7/10
A	EP 0 610 886 A (MITSUBISHI ELECTRIC CORP) 17. August 1994 (1994-08-17) * Spalte 3, Zeile 56 - Spalte 6, Zeile 34 *	1	
A	US 5 491 827 A (HOLTEY THOMAS O) 13. Februar 1996 (1996-02-13) * Spalte 2, Zeile 55 - Spalte 4, Zeile 26 *	1	

RECHERCHIERTE SACHGEBIETE (Int.Cl.6)

G06K
G07F

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
DEN HAAG	19. Juni 2002	Goossens, A

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 99 20 0263

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

19-06-2002

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
EP 0512542	A	11-11-1992	DE	4115152 A1	12-11-1992
			AT	148953 T	15-02-1997
			DE	59208026 D1	27-03-1997
			DK	512542 T3	18-08-1997
			EP	0512542 A2	11-11-1992
			ES	2100249 T3	16-06-1997
			HK	1007818 A1	23-04-1999
			JP	5173890 A	13-07-1993
			US	5600818 A	04-02-1997
EP 0610886	A	17-08-1994	JP	6236447 A	23-08-1994
			DE	69428616 D1	22-11-2001
			EP	0610886 A2	17-08-1994
			US	5506396 A	09-04-1996
US 5491827	A	13-02-1996	AT	206543 T	15-10-2001
			CA	2158265 A1	20-07-1995
			CN	1122164 A ,B	08-05-1996
			DE	69522998 D1	08-11-2001
			DE	69522998 T2	13-06-2002
			DK	689702 T3	03-12-2001
			EP	0689702 A1	03-01-1996
			ES	2164144 T3	16-02-2002
			FI	954299 A	13-09-1995
			WO	9519608 A1	20-07-1995
			JP	2755828 B2	25-05-1998
			JP	8506915 T	23-07-1996
			KR	205740 B1	01-07-1999
			NO	953614 A	13-11-1995
			SG	49773 A1	15-06-1998
			TW	432283 B	01-05-2001

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82